REMARKS

Applicant respectfully requests reconsideration of this application, as amended, and consideration of the following remarks. Claims 1, 14 and 19 have been amended. Claims 5, 6, 11, 13, 15-17 were previously canceled. New claims 22 and 23 have been added. Claims 1-4, 7-10, 12, 14 and 18-22 remain pending.

Claims 1-4, 7-10, 12, 14 and 18-21 stand rejected under 35 U.S.C. 112, first paragraph as failing to comply with the written description requirement.

Claims 1-4, 7-10, 12, 14 and 18-21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Zakiya (U.S. Pat. Pub. 2002/0032551) in view of Qi (U.S. Pat. Pub. 2002/0184498) and further in view of Oklobdzija ("A Method for Speed Optimized Partial Product Reduction and Generation of Fast Parallel Multipliers Using an Algorithmic Approach" IEEE Transactions on Computers, Vol. 45, No 3, March 1996. Vojin G. Oklobdzija et al.).

Amendments

Amendments to the Claims

Applicant has amended the claims to more particularly point out what Applicant regards as the invention. No new matter has been added as a result of these amendments as they were supported elsewhere in the specification, claims and drawings as originally filed.

December 9, 2208 Telephone Interview

Applicant thanks the Examiner for his time and patience in discussing the invention with the Inventor Rarick and the undersigned on December 9, 2008. While no specific agreements with regard to allowance were reached the discussions reviewed the differences and the importance thereof between 4 to 2 compressors and full adders.

Rejections

Rejections under 35 U.S.C. §103(a) and 112, First Paragraph

Claims 1-4, 7-10, 12, 14 and 18-21 stand rejected under 35 U.S.C. 112, first paragraph as failing to comply with the written description requirement. Claims 1-4,

7-10, 12 and 14 and 18-20 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Zakiya (U.S. Pat. Pub. 2002/0032551) in view of Qi (U.S. Pat. Pub. 2002/0184498). Applicant respectfully traverses these rejections as set forth in more detail below.

Inventor Leonard D. Rarick's declaration under 37 CFR 1.132, submitted herewith, more specifically describes the difference and the advantages and the reasons why the 4 to 2 compressor has not been used in cryptographic processors before. Further, the inventor declares that the 4 to 2 compressor has a 3 gate delay that the "4 to 2 compressors are defined in the art of multiplier arrays to have a ***3 XOR gate delay.***"

Therefore Applicant submits the rejection of claims 1-4, 7-10, 12, 14 and 18-21 under 35 U.S.C. 112, first paragraph as failing to comply with the written description requirement has been overcome and the 35 U.S.C. 112 rejection should be withdrawn.

The Zakiya reference discloses methods and systems to perform hash algorithms as logic gate functions. It processes an N-bit block of data into the M-bit hash or message digest of the block in one (1) process cycle instead of the multiple cycles generally required. The minimum process time is the total propagation delay of an input block through the core logic for an implementing technology. A message requiring Y blocks to process would require no more than Y process (clock) cycles to produce the final hash value. This creates very simple and fast implementations of hash algorithms which enable them to be simply and easily integrated into any system.

The Qi reference discloses an architecture (hardware implementation) for an authentication engine to increase the speed at which SHA1 multi-loop and/or multi-round authentication algorithms may be performed on data packets transmitted over a computer network. As described in this application, the invention has particular application to the variant of the SHA1 authentication algorithms specified by the IPSec cryptography standard. In accordance with the IPSec standard, the invention may be used in conjunction with data encryption/encryption architecture and protocols. However it is also suitable for use in conjunction with other non-IPSec

cryptography algorithms, and for applications in which encryption/decryption is not conducted (in IPSec or not) and where it is purely authentication that is accelerated. Among other advantages, an authentication engine in accordance with the present invention provides improved performance with regard to the processing of short data packets.

Oklobdzija describes a multiplier array using a 4 to 2 compressor and describing the 4 to 2 compressor has a propagation logic delay of 3 XOR gates where two sequential full adders have a propagation logic delay of 4 XOR gates.

Zakiya's carry look-ahead adders (for example, instead of 340 and 341 in Figure 3 or instead of 540 and 541 in Figure 5 or instead 740 and 742 in Figure 7) which are much longer propagation delay and consume much more area of the die than a 4 to 2 compressor.

Qi uses two, sequential 3 to 2 compressors (usually called full adders, or FA as shown in Qi's Figures 6A, 7, 9A, 9B, and 10) instead of using Applicant's 4 to 2 compressors.

Qi's two, sequential 3 to 2 compressors consumes the approximately the same area as the Applicant's 4 to 2 compressors, however, Qi's two, sequential 3 to 2 compressors have a 33% longer propagation delay.

The Examiner states that Qi's Figure 9B shows a 4 to 2 compressor. However, this is not a 4 to 2 compressor and even Qi does not call it that. Qi's paragraph [0059] provides as follows:

> "[0059] Two comprehensive addition modules, add5to1 and add4to1, in the architecture each use several stages of CSA followed-by a carry look-ahead (CLA) adder, as illustrated and described in more detail with reference to FIG. 10, below. **FIGS. 9A and 9B illustrate block diagrams of the add5to1 and add4to1 comprehensive addition modules, respectively**. The add5to1 module includes three CSA adders followed by a CLA. **The add4to1 module includes two CSA adders followed by a CLA**." (Emphasis added)

Qi clearly refers to this module as a "comprehensive addition module". Qi further describes the comprehensive addition module as "The add 4 to1 module includes two CSA adders followed by a CLA."

Applicant submits that two CSA adders (full adders) in sequence is ***not*** the same thing as a 4 to 2 compressor. Each CSA (full adder, see Qi's Fig. 6A) has the minimum propagation delay latency of two XOR gates and so two CSAs in sequence have the minimum propagation delay latency of ***four XOR gates***.

Applicant's 4 to 2 compressor is NOT just "any circuit unit that receives multiple inputs and compresses them into fewer outputs". By way of example, Applicant's 4 to 2 compressor has the ***constant*** propagation delay latency of ***only three XOR gates*** as compared to the propagation delay latency of Qi's circuit.

Applicant's 4 to 2 compressor also has a propagation latency that is ***independent*** of the vector length where the structures of both Qi and Zakiya are have propagation latencies ***dependent*** on the vector length. Restated, both Qi and Zakiya has a propagation latency that increases as the number of bits in the vector being processed increases. Applicant's 4 to 2 processor has a fixed propagation latency of 3 XOR gates regardless of the number of bits in the vector being processed.

The propagation latency of Applicant's 4 to 2 compressor from the inputs to the outputs of a compressor is independent of length of the vectors. It does not matter how many terms are in the vector (the range of the variable i), the execution time of Applicant's 4 to 2 compressor is constant.

In sharp contrast, Qi's Figure 8 shows a carry look-ahead adder. The carry value must propagate the entire length of the carry look-ahead adder circuit from C0 to Ci+1 in the Carry look-ahead Logic.

Therefore, as the size of the vectors increase (i.e., as the value of i increases), not only does the width of the Carry Look-ahead Logic increase, but the depth (the vertical height) of the Carry Look-ahead Logic also increases and as a result, the propagation delay also increases with the log of the vector size.

Therefore, Qi's Carry Look-ahead Logic does not have a ***constant*** propagation latency that is independent of the size of the vector, where Applicant's 4 to 2 compressor does have a constant propagation latency of 3 XOR gate delays that is entirely independent of the size of the vector.

While Qi does use full adders Qi does not teach or suggest using 4 to 2 compressors as Applicant does (i.e., having Applicant's smaller size and reduced, constant propagation latency). Further, Qi does not teach or suggest a circuit that is capable of executing multiple hash algorithms.

Turning to Zakiya, Zakiya does not show any compressors in any of Zakiya's figures since two inputs summed to one output necessarily involves carries propagating the carry along the length of the vector which cannot be done in constant (vector length independent) latency propagation delay.

Thus, much as described above with regard to Qi's structure, Applicant submits that Zakiya's carry look-ahead adder is not the same as nor even suggestive of Applicant's 4 to 2 compressor.

Further, Zakiya does not use any type of compressor circuit. As a practical matter, this makes Zakiya's circuits much larger in area and slower, vector length dependent, propagation delay than Applicant's system with a constant vector length independent, propagation delay.

The combination of Qi and Zakiya will not resolve the failings of the teachings of the references when considered alone. For example, referring to Qi's Figure 9B and substituting that structure in for modules 340, 341, and 342 in Zakiya's Figure 3 would result in 342 in Zakiya's Figure 3 being the same as the CLA in Qi's Figure 9B. This may be a substantial improvement over either Qi or Zakiya separately, but still not as good as using Applicant's further reduced propagation latency that is also a vector length independent propagation latency and also provides a smaller area consumption afforded by Applicant's 4 to 2 compressor.

It would not be obvious to add a vector length independent propagation latency structure to either Qi or Zakiya or a combination thereof because both Qi and Zakiya utilize the vector length ***dependent*** propagation latency structures and this impacts the design and timing of the entire structure.

Applicant submits that neither Zakiya nor Qi teach or even suggest a 4 to 2 compressor in a hash logic circuit on in any other circuit. Oklobdzija describes a 4 to 2 compressor in the ***context of a multiplier array***.

Even though Oklobdzija dates from 1996, no one has applied a 4 to 2 compressor to processors like a cryptographic processor at least in part due to the only slight improvement in logic propagation time delay from 4 XOR gate delays to a 3 XOR gate delays.

Inventor Leonard D. Rarick's declaration under 37 CFR 1.132, submitted herewith, more specifically describes the difference and the advantages and the reasons why the 4 to 2 compressor has not been used in cryptographic processors before.

Motivation to improve semiconductor circuit design such as microprocessors and encryption processors, including the hash logic as described in the present application, is driven by power, semiconductor die area or reduction in logic delay. Comparing a 4 to 2 compressor to two sequential full adders shows approximate equal device count, semiconductor die area and power consumption and ***only a single*** XOR gate delay reduction. 4 to 2 compressors were developed in the art of multiplier arrays because the longest column in the multiplier array uses several 4 to 2 compressors, for example a 64 X 64 multiply array with Booth encoding uses at least four 4 to 2 compressors arranged sequentially (12 XOR gate delay total) to replace eight sequential full adders (16 XOR gate delay total). By way of example in a multiplier array, using four 4 to 2 compressors arranged sequentially ***yields a 4 XOR gate delay improvement*** as compared to using eight sequential full adders.

If a processor (e.g., microprocessor and/or encryption processor) die area and power consumption is not changed and the logic delay of a portion (e.g., hash logic) of the processor is only slightly reduced, Applicant submits ***there is substantial motivation to***

not change that portion of the processor because that slight reduction in logic delay could require significant redesign of adjacent portions of the processor to compensate for the slight reduction in logic delay.

Using the 4 to 2 compressors in a multiplier array reduces the latency of each column in the multiplier array by ***multiple XOR gate delays*** as compared to using sequential full adders. In a multiplier array the delay of each column can be additive and therefore the reduced logic delay of each column can yield a further reduced logic delay of the entire multiplier array.

Therefore there is substantial motivation to use 4 to 2 compressors in multiplier arrays. Applicant submits that same motivation to use 4 to 2 compressors ***does not exist*** in a cryptographic processor design as the change caused by making the minor improvement in timing (a single XOR gate delay) can necessitate substantial redesign in other portions of the processor.

Applicant submits that this added redesign for very little gain ***teaches away from*** the type of improvements criteria (power, area, speed) typically applied to improving processors and therefore submits that Oklobdzija teaches away from being combined with either of Qi or Zakiya or a combination thereof.

As to claims 1-4, 7-10, 12, 14 and 18-20, none of the cited references whether considered alone or in combination teach or suggest a system method or apparatus where the hash modules share logic components (e.g., adders, compressors, etc.) that are selectable and used to perform the respective, selected hash functions. Nor do any of the cited references whether considered alone or in any combination teach or suggest a hash module that includes a 4 to 2 compressor.

With regard to new claim 21 and amended claims 14 and 19, neither of Qi or Zakiya or Oklobdzija or any combination thereof nor any of the previously cited references whether considered alone or in any combination teach or suggest a cryptographic algorithm unit including a first-cryptographic hash execution module that is capable of executing at least one of a group of cryptographic hash algorithms consisting of a SHA256 hash algorithm, a SHA384 hash algorithm, and a SHA512

hash algorithm and a second cryptographic hash execution module is capable of executing at least one of a group of cryptographic hash algorithms consisting of the SHA-1 hash algorithm, a SHA256 hash algorithm, a SHA384 hash algorithm, and a SHA512 hash algorithm that is different from the cryptographic hash algorithm than the first cryptographic hash execution module is capable of executing.

With regard to new claim 22 none of the cited references nor any of the previously cited references whether considered alone or in any combination teach or suggest a cryptographic hash execution module, including a four to two compressor wherein the four to two compressor has a vector length independent logic propagation delay of less than four XOR gates. Claim 23 depends from claim 22 and is patentable of the cited art for at least the same reasons as set forth for claim 22.

Accordingly, Applicant respectfully submits that Applicant's invention as claimed in claims 1-4, 7-10, 12, 14 and 18-23 is patentably distinct over any of the cited references whether considered alone or in any combination, and respectfully request the withdrawal of the rejections under 35 U.S.C. §103(a) and 112.

SUMMARY

In view of the foregoing amendments and remarks, Applicant respectfully submits that the pending claims are in condition for allowance. Applicant respectfully requests reconsideration of the application and allowance of the pending claims.

If the Examiner determines the prompt allowance of these claims could be facilitated by a telephone conference, the Examiner is invited to contact George B. Leavell at (408)774-6923.

Deposit Account Authorization

Authorization is hereby given to charge our Deposit Account No. 50-0805 (Ref SUNMP349) for any charges that may be due or credit our account for any overpayment. Furthermore, if an extension is required, then Applicant hereby requests such extension.

Respectfully submitted,

MARTINE PENILLA & GENCARELLA, LLP

Dated: February 13, 2009

/George B. Leavell/

George B. Leavell
Attorney for Applicant
Registration No. 45,436
710 Lakeway Drive, Suite 200
Sunnyvale, CA 94085
(408) 774-6923